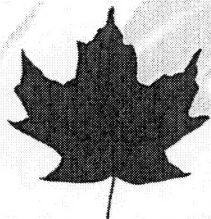




Immigration, Refugees
and Citizenship Canada

Immigration, Réfugiés
et Citoyenneté Canada

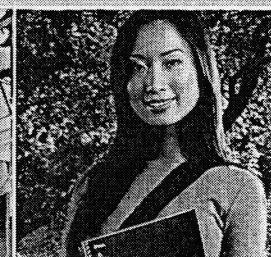
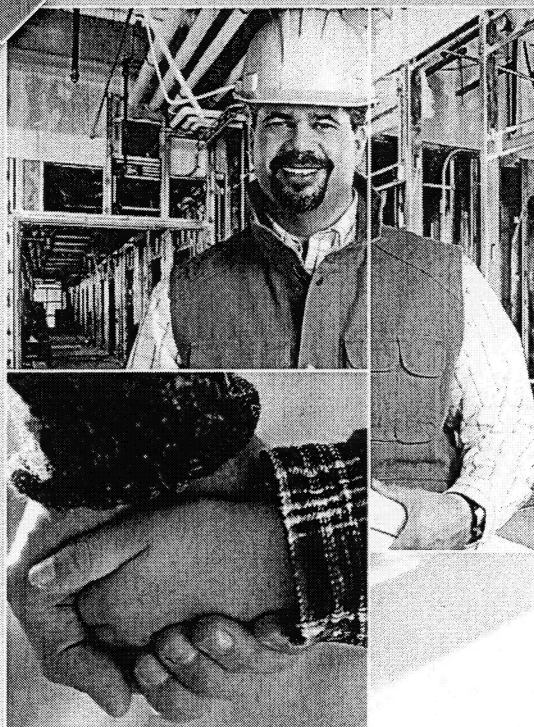
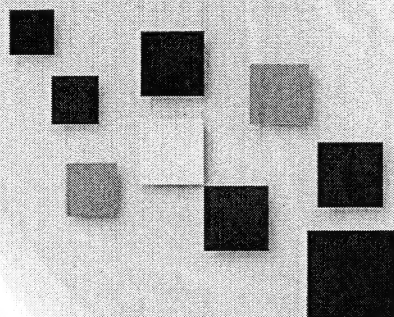


Privacy Impact Assessment

Migration Five Information Sharing Regulations



Immigration, Refugees and Citizenship Canada



IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

Name of Branch/Division:	Admissibility – Identity Management and Information Sharing		
PIA Drafter:	Brad Adams-Barrie		
Email:	Bradley.Adams-Barrie@cic.gc.ca	Phone:	613-437-7890
Program Manager:	Emmanuelle Deault-Bonin		
Email:	Emmanuelle.Deault-Bonin@cic.gc.ca	Phone:	613-437-5894

Part 1 – General Information

1. Description of the Initiative

The Migration Five (M5) is a longstanding forum for cooperation between the border and immigration agencies of Australia, Canada, New Zealand, the United Kingdom (UK), and the United States (U.S.). Given the commonalities among our immigration programs, the exchange of immigration information among M5 partners is a particularly beneficial element of this cooperation.

While manual and case-by-case information exchanges with M5 partners have proven to be a valuable tool for immigration decision-makers, the labour-intensive process involved has limited the number of cases for which information exchanges may take place. These manual, case-by-case exchanges are undertaken pursuant to section 8(2) of the *Privacy Act*, as well as case-by-case arrangements with each M5 partner.

In 2015, Canada began automated, biometric-based immigration information exchanges with the U.S., supported by regulatory amendments that were enacted to enable (though not require) these exchanges. In 2017, Canada is establishing a similar automated capability to exchange immigration information with its remaining M5 partners, namely Australia, New Zealand, and the UK. This Privacy Impact Assessment (PIA) covers the regulatory amendments that have been brought forward to provide a reasonable lawful authority for biometric-based immigration information sharing with these three partners.

While the M5 is a *multilateral* forum for cooperation, information exchanges between each country occur on a *bilateral* basis. Automated biometric-based immigration information sharing refers to an automated query and response process whereby the exchange of information is triggered when either Canada or an M5 partner sends a client's encrypted and anonymous fingerprints, plus the case type (e.g., visa applicant, refugee claimant, etc.) to the other country.

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

The case type is included as part of the query to enable the exchange of information on permanent residents for refugee cases only. Under no circumstance will the client's identity be disclosed as part of the query. The country receiving the query will search its relevant database for a fingerprint match. Regardless of the result (*i.e.*, whether or not there is a match), the receiving country will automatically and immediately delete the encrypted fingerprints used in a query. In the case of a match, the receiving country will reply with limited and agreed-to data elements, consisting of biographic identity information and immigration information. Officials in each jurisdiction can use the shared information to inform their independent admissibility decisions on the basis of their own country's immigration and refugee protection laws.

For Canada, fingerprint queries will be submitted to an M5 partner to support an examination or determination following an application or claim made by a national of a third country for a permanent or temporary resident visa, a work or study permit, protection, refugee protection or any other immigration benefit, or to determine whether the national of a third country is authorized to travel to, enter or remain in Canada (Sub-section 315.4(1) of the Regulations). It is expected that Canada will have the ability to send up to 400,000 queries per year to each of these three countries, for a total of 1.2 million queries per year. It is important to note that while these regulations enable automated information sharing, they do not create a requirement to share information.

At the same time, M5 partners will query Canada for similar purposes, and Canada will disclose information in response to a query in order to support an M5 partner's examination or determination following an application or claim made by a national of a third country for a visa or immigration-related permit, status or benefit, or to determine whether the national of a third country is authorized to travel to, enter or remain in the M5 partner's territory (Paragraphs 315.41.1(a) and (b) of the Regulations). It is expected that each of these three countries will have the ability to send Canada up to 400,000 queries per year.

Canada will not disclose information on Canadian citizens. However, in order to uphold Canada's international commitments related to refugees, Canada may disclose information on Canadian permanent residents only in response to a query on a refugee case, to indicate to a partner that the individual in question has a durable solution in Canada. (Paragraph 315.41(1)(d) of the Regulations).

2. Scope of this Privacy Impact Assessment

This PIA covers automated, biometric-based immigration information sharing with Australia, New Zealand, and the UK, as enabled by amendments to the *Immigration and Refugee Protection Regulations* (IRPR). For ease of reference, the regulatory authority for this information sharing can be found beginning at Section 315.36 of the IRPR.

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

As the Regulations apply to automated biometric-based immigration information sharing with these three countries, separate PIAs will not be developed for each of the Automated Annexes to the Memoranda of Understanding (MOU) with each M5 partner, as the information sharing activities thereunder are governed by the Regulations. If, during negotiations, significant differences arise in either the contemplated exchange of information between Canada and an M5 partner, or the specific data being exchanged between Canada and an M5 partner, addenda to this PIA will be provided in order to account for notable differences.

This PIA does not cover:

- the storage of information in Immigration, Refugees and Citizenship Canada's (IRCC) Global Case Management System (GCMS), for which a PIA was submitted in 2011;
- the MOUs with Australia, New Zealand or the UK, nor the related Case-by-Case Annexes, for which PIAs were submitted in 2015 for the UK and 2016 for Australia and New Zealand;
- the High Value Data Sharing Protocol, for which a PIA was submitted in 2012; or,
- the role of the Royal Canadian Mounted Police (RCMP) as the service provider for IRCC's biometric program, for which the RCMP will submit a PIA in 2017.

3. Legal Authorities

The legislative authority for establishing information sharing regulations is:

Immigration and Refugee Protection Act

Sub-paragraphs 150.1(1)(a) and 150.1(1)(b)

150.1 (1) The regulations may provide for any matter relating to

- (a) the collection, retention, use, disclosure and disposal of information, including a Social Insurance Number, for the purposes of this Act or for the purposes of program legislation as defined in section 2 of the Canada Border Services Agency Act;
- (b) the disclosure of information for the purposes of national security, the defence of Canada or the conduct of international affairs, including the implementation of an agreement or arrangement entered into under section 5 or 5.1 of the Department of Citizenship and Immigration Act or section 13 of the Canada Border Services Agency Act;

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

4. Related Privacy Impact Assessments

The operational and technical infrastructure being developed to support information sharing with M5 partners is as described in the *Addendum Privacy Impact Assessment Report covering Biometric Systematic Information Sharing between Canada and the United States*, which was submitted to the Office of the Privacy Commissioner in May 2015.

At this time, there is one substantive privacy-linked difference between the existing automated biometric-based information sharing program in place with the United States and the program being established with the remaining M5 partners.

Specifically, Australia's Department of Immigration and Border Protection has expressed an interest in querying Australian citizenship applicants against Canada's immigration-related biometric records. This means that Canada may provide limited immigration information to Australia on a national of a third country that would be used by Australia to support a citizenship-related examination or determination. This variance is captured at Paragraph 315.41(1)(c) of the regulations.

For clarity, Canada will not send queries to M5 partners on individuals applying for Canadian citizenship.

5. Elements of Information or Data

When querying an M5 partner, IRCC will submit the person's fingerprints accompanied by a unique transaction number (Section 315.38 of the Regulations).

In the event that a query received from an M5 partner results in a fingerprint match in Canada's immigration-related biometric database, Canada will disclose:

- the individual's biographic data, such as last name, first name, date of birth, gender and country of birth;
- their photograph; and,
- information related to the administration and enforcement of Canada's immigration laws, including the issuing country of the individual's passport, the individual's immigration status, information relevant to – and any previous decision or determination relating to – their admissibility, and any decision or determination relating to a claim for refugee protection or an application for protection (Paragraphs 315.41(2)(a), 315.41(2)(b), and 315.41(2)(c) of the Regulations).

As described in section 4, Australia's Department of Immigration and Border Protection has expressed an interest in querying Australian citizenship applicants against Canada's immigration-related biometric records. This means that Canada may provide limited immigration information to Australia on a national of a third country which would be used in supporting a citizenship-

IRCC Privacy Impact Assessment

Migration Five Information Sharing Regulations

related examination or determination (Paragraph 315.41(1)(c) of the Regulations). Canada will not send queries to M5 partners on individuals applying for Canadian citizenship.

While the regulations list the information categories that may be disclosed by Canada, the following exhaustive list of data elements may be provided in response to all biometric matches, subject to availability:

- Providing Participant subject specific reference number;
- Providing Participant event specific reference number;
- Name(s);
- Alias(es);
- Gender;
- Photograph / Facial image;
- Date of birth;
- Passport Nationality or nationalities;
- Country of birth;
- Travel document information, including scans of documents;
- Current and previous Immigration status;
- Location(s), date(s) and reason(s) fingerprinted;
- Country of Alleged Persecution;
- Reason for alert;
- Visa refusal code(s);
- Watchlist indicator;
- Date(s) and location(s) of arrival;
- Date(s) and location(s) of departure;
- Date removed;
- Status of a refugee claim;
- Date(s) of immigration application;
- Type(s) of immigration application;
- Date(s) of outcome of immigration application;
- Outcome of immigration application;
- Reason for outcome of immigration application;
- Expiry date of current leave/stay or visa.

Business rules in GCMS preclude disclosures described in paragraph 315.41(3) of the regulations, i.e., disclosures inconsistent with domestic law or national interests.

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

6. Storage or Access outside Canada

Information disclosed by Canada to Australia, New Zealand or the UK in response to a query will be retained in accordance with the terms of the respective MOU, Automated Annex, and Australian, New Zealand, or UK law.

Information disclosed to Australia's Department of Immigration and Border Protection will be stored in Australia's Biometric Acquisition Matching Service system.

Information disclosed to New Zealand's Ministry of Business, Innovation and Employment will be stored in New Zealand's "M5 Check" system.

The UK's Home Office is currently undertaking an overhaul of its immigration information technology systems, and automated biometric-based information sharing is not scheduled to be implemented between Canada and the UK until 2018 at the earliest. Clarification will be sought by Canada at that time as to which system the UK will store information received from Canada.

Officials in Australia, New Zealand, or the UK will not have direct access to Canadian case files, databases or other information held by IRCC, or vice versa.

The information IRCC receives from Australia, New Zealand, or the UK will be stored in GCMS, which is housed in Canada. Information may also be kept on client case files in paper format.

7. Data-matching program

Answer the following questions to determine whether your initiative qualifies as a "data-matching program". If you answer "yes" to all 3 questions, your initiative may be a data matching program.

1. Personal information from one database is linked or combined with personal information from another database;	Yes
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	No
3. The linkage results in an administrative decision about an individual.	Yes

If you have answered "yes" to all three questions, please contact ATIP Division to discuss the requirements of a data-matching program.

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

8. Multi-institutional/Multi-jurisdictional

Is your initiative Multi-institutional/ Multi-jurisdictional ? Will the privacy impact assessment involve more than one government institution? <i>YES – IRCC and the CBSA are both subject to the Immigration and Refugee Protection Regulations, including the information sharing regulations being examined in this PIA report.</i>	
1. This initiative involves a program or activity that provides a service (or services);	Yes
2. Those services are provided through: (a) an institution and at least one other institution or department working collaboratively to provide that service; or (b) one institution working on behalf of one or more other institutions;	Yes
3. The common or integrated program/activity is confirmed by written documentation.	Yes
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	<input checked="" type="checkbox"/>

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

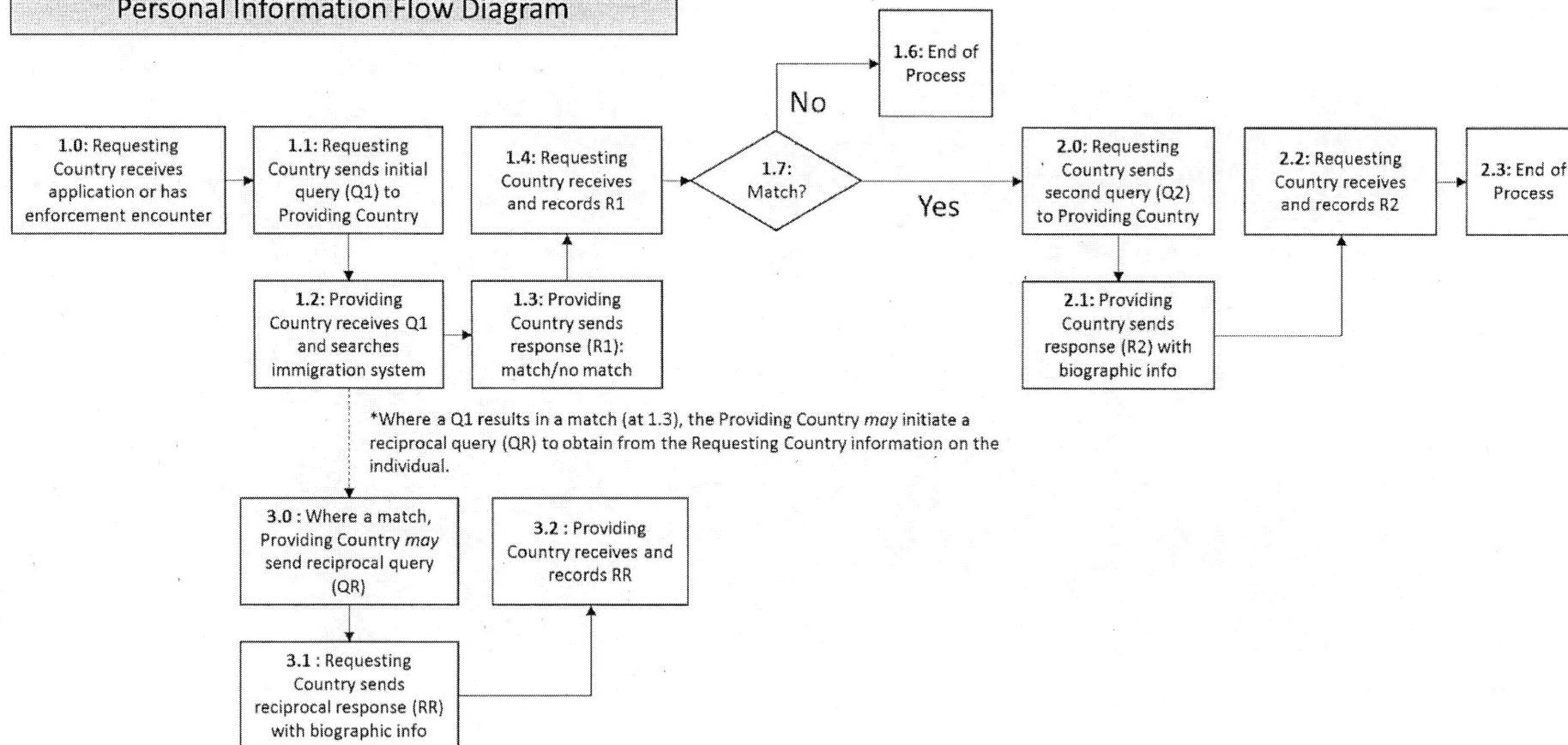
Part 2 – Protection of Personal Information

9. Personal Information Flow Diagram and/or Personal Information Flow Table

A data flow diagram is provided below outlining the automated search and response process. The following information can be used as a reading guide for the data flow diagram.

- The requesting country initiates a query using an anonymous electronic fingerprint. (see section 1.0 in data flow diagram).
- The anonymous fingerprint is searched against the providing country's applicable database.
- If a match is established, the providing country responds with biographic information (*e.g.*, name, age, nationality, etc.) and limited immigration information (*e.g.*, reason fingerprinted).
- The fingerprint is deleted by the providing country.
- Following a match, the requesting country requests additional immigration information from the providing country. (see section 2.0 in data flow diagram).
- The providing country automatically provides additional immigration information, subject to availability (*e.g.*, travel document information; application outcomes).
- The providing country can also send a "reciprocal query" in specific and limited circumstances to receive identity information and limited immigration data to assist in administering and enforcing its own immigration laws (*e.g.*, when the query hits against an open immigration warrant). (see section 3.0 in data flow diagram).

Automated Biometric-based Information Sharing: Personal Information Flow Diagram



IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

10. Disclosure Notice

Immigration application forms include a disclosure notice indicating the authority for, and purpose of, the collection of information and how to obtain further information on applicable Personal Information Banks. Immigration application forms also state that personal information, including immigration information related to biometric records, may be shared with foreign governments with whom Canada has an agreement or arrangement. IRCC application forms are available via the following link: <http://www.cic.gc.ca/english/information/applications/>.

Of note, IRCC is presently undertaking a review of disclosure notices on application forms linked to its biometrics program and will seek to ensure compliance with the Directive on Privacy Practices where gaps are identified.

Part 3 – Security of Personal Information

11. Describe the physical security measures related to the initiative.

Information exchanged under the regulations will be securely stored and encrypted in accordance with existing Government of Canada security procedures and standards.

12. Describe the technical security measures related to the initiative.

Encryption

Information collected from and disclosed to Australia's Department of Immigration and Border Protection, New Zealand's Ministry of Business, Innovation and Employment, or the UK's Home Office will be protected with controls and safeguards applicable to Protected 'B' information, including encryption during electronic transmission. Details regarding the encryption of automated biometric-based information sharing is available in the Addendum Privacy Impact Assessment Report covering Biometric Systematic Information Sharing between Canada and the United States.

Controlled User Access Profiles

GCMS Access Controls allow users who have the proper authorization to obtain access to specific items of information. Credentials are used to verify and authenticate the identity of these users where special permission and authorizations are required to perform tasks and processes. GCMS users are assigned access to the system by role and office based on their specific job requirements. Information received from an M5 partner is captured in a specific GCMS view, to which access is limited to IRCC and CBSA employees with an immigration case processing role. For more detailed information regarding GCMS access controls, please refer to the GCMS PIA that was submitted to the Office of the Privacy Commissioner in 2011.

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

13. Does your branch rely on security policies in addition to the TBS Policy on Government Security?

IRCC adheres to Canadian laws and policies guiding the protection of personal information. In addition to the TBS policy on Government Security, IRCC adheres to the TBS Operational Security Standard on Physical Security which provides baseline physical security requirements for the storage, transmittal, and destruction of classified and protected information. IRCC will also adhere to the CSE's *IT Security Risk Management: A Lifecycle Approach* (ITSG-33) guidelines which provide a set of clearly defined activities to ensure key steps are performed on an ongoing basis during the lifetime of the department's information systems, and to ensure risk management is applied from an enterprise perspective. Per CSE's ITSG-33 guidelines, IRCC performs the Security Assessment & Authorization (SA&A) process, resulting in a signed Authority to Operate (ATO) for every GCMS release, including those through which automated biometric-based information sharing has been or will be implemented with Australia, New Zealand and the UK.

- *Operational Security Standard on Physical Security*
<http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329§ion=text#appB>
- *IT Security Risk Management: A Lifecycle Approach (ITSG-33)*
<https://www.cse-cst.gc.ca/en/node/265/html/22814>

14. Describe any mitigating access controls to limit or restrict unauthorized access to personal information including changes such as additions or deletions.

Personal information may only be accessed by authorised individuals who have a need to access that information in performing their official duties. Only specific IRCC and CBSA officials may access information received from Australia's Department of Immigration and Border Protection, New Zealand's Ministry of Business, Innovation and Employment, or the UK's Home Office.

Exchanges will be recorded in GCMS, where additions or deletions are subject to user controls. Furthermore, all automated exchanges of information will be immediately marked and labeled on the client's file in GCMS. The special treatment of this information within GCMS will further emphasize the controlled nature of this information and more readily allow, in the case of access to information requests, for an individual to know that an information exchange was completed with Australia, New Zealand, or the UK.

15. Explain how you will identify individuals accessing personal information without authorization.

GCMS Access Controls allow users who have the proper authorization to obtain access to specific items of information. Access Control processes are in place to restrict read/write access to GCMS data (which includes any biometric related data stored in the GCMS system).

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

The auditing controls collect data, support analysis, and manage the archiving of all information. The auditing controls allow for the capture, analysis, and retrieval of records of events and conditions within a computing solution.

Data Auditing is divided into Write Auditing and Read Auditing. Read audit refers to the ability to capture which GCMS user has viewed data and the content of the data at that point in time. Write audit refers to the capturing of changes to data that occur within the GCMS system. The goal of the write audit is to capture what changes, additions and deletions are performed on the system, which user performed the changes and when they occurred. The write audit requirements being addressed by GCMS can be expressed as the ability to answer the following questions:

- What activity did a given user perform over a specified time period;
- What activity was performed against a given client over a specified time period; and
- What activity against a given client was performed by a given user over a specified time period?

Audit can be in real-time, such as an Intrusion Detection system, or can be after the fact, such as a scheduled periodic review of events that have been previously gathered in a log. Audit Controls include:

- collection of audit data about events, including capture of the appropriate data, trusted transfer of audit data, and synchronisation of chronologies;
- protection of security audit data, including use of time stamps, signing events, and storage integrity to prevent loss of data;
- analysis of security audit data, including review, anomaly detection, violation analysis, and attack analysis using simple or complex heuristics; and
- alarms for event or activity thresholds, warning conditions, and critical events.

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

Part 4 – Accuracy/Correction/Retention of Personal Information

- 16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the Department notify them of the update, correction or annotation?**

IRCC will use existing processes to respond to requests for access to information made under the *Access to Information Act*, and the correction of inaccurate information under the *Privacy Act*.

If an individual has a right of access to his or her information under the *Privacy Act* and makes a request regarding corrections to said information, IRCC will comply as appropriate.

If IRCC or the CBSA becomes aware that information disclosed in response to a query from an M5 partner is inaccurate, the recipient of the inaccurate information must be notified and correcting information be provided as soon as feasible (Sub-section 315.42(1) of the Regulations). Similarly, if IRCC or the CBSA receives information from an M5 partner that corrects information previously disclosed by that partner, IRCC or the CBSA must make the necessary correction as soon as is feasible and notify the partner that the correction has been made (Sub-section 315.42(2) of the Regulations).

- 17. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.**

Yes. Personal information may be used to inform immigration and refugee decisions, and in the case of Australia, decisions related to Australian citizenship applications. Biometric-based information sharing can help verify a client's identity and obtain previously unknown immigration information.

- 18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.**

Where personal information is collected directly from the client, it is incumbent on the client to provide information that is accurate and complete. When clients provide new and updated information, it can be entered and reflected in GCMS.

IRCC and its counterparts in M5 countries are committed to providing the most up to date and accurate information available. If Canada or an M5 partner becomes aware that the other is using inaccurate information, there is an obligation to notify the other immediately and provide correct information, where available. As described in section 16, Canada's obligation to correct inaccurate information disclosed in response to a query is captured in the regulations; information disclosed in either a query or response is limited to that which is necessary, relevant and proportionate to

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

achieving the purposes of the Regulations, and the information must be disclosed in a manner that ensures the accuracy and reliability of the information (Section 315.39 of the Regulations).

- 19. If you answered “yes” to question 17, do you have approved records retention and disposition schedules that will ensure that personal information is kept for a minimum of two years after it is used in making a decision directly affecting an individual?**

Yes. Domestic retention policies and laws apply to the information exchanged under the authority of the regulations (Sub-section 315.43(1) of the Regulations, with the exception of the fingerprints used to form the query, which are always deleted by the receiving partner regardless of outcome (Sub-section 315.13(2) of the Regulations).

Information will be retained in accordance with the approved records retention and disposition schedule for the relevant application type.

Part 5 – Further Information

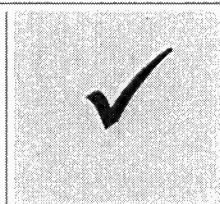
- 20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.**

Yes. Personal information will be disclosed in an automated and systematic manner as described in section 9.

For Canada, queries will be automated and initiated upon receipt of an application or claim for which the applicant is required to submit biometrics (i.e. fingerprints).

Canada’s responses to queries from an M5 partner will also be automated. When a fingerprint match has been established by the RCMP, IRCC will pull the limited and relevant immigration information from the client’s file in GCMS and return the data elements listed in question 5, as available, to the applicable M5 partner.

Please check this box if a related Information Sharing Agreement (ISA) has been prepared. If you have general questions about preparing an ISA, please contact your International and Intergovernmental Relations (IIR), Intergovernmental Relations (IGR) at NHQ-IGR@cic.gc.ca - or contact the ATIP division at ATIPinternal-AIPRPinterne@cic.gc.ca .



IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

If an ISA has been prepared as part of your initiative, please complete the fields in the table below.

Information Sharing Agreement – Required Information	
Description	<p>Annex to the Memorandum of Understanding between the Department of Citizenship and Immigration Canada and the Canada Border Services Agency and the Department of Immigration and Border Protection of Australia regarding the Exchange of Information on an Automated Basis;</p> <p>Annex to the Memorandum of Understanding between the Department of Citizenship and Immigration Canada and the Canada Border Services Agency and New Zealand's Ministry of Business, Innovation, and Employment (Immigration New Zealand) regarding the Exchange of Information on an Automated Basis.</p> <p><i>N.B.:</i> A Canada-UK Annex for the automated exchange of information is currently under development.</p>
Primary government institution involved	IRCC and CBSA and, on a bilateral basis, Australia's Department of Immigration and Border Protection & New Zealand's Ministry of Business, Innovation and Employment, and the UK's Home Office.
All other government institution and/or parties involved	N/A
ISA contact title	IRCC – Emmanuelle Deault-Bonin, A/Director, Identity Management and Information Sharing CBSA – Sébastien Aubertin-Giguère, A/Director General, Traveller Program Directorate
ISA contact telephone number	Emmanuelle Deault-Bonin: 613-437-5894 Sébastien Aubertin-Giguère: 613-952-3266
Indication of whether or not personal	Yes, the exchange of personal information is

IRCC Privacy Impact Assessment

Migration Five Information Sharing Regulations

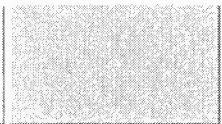
information is involved	involved in this arrangement.
Start date	The Canada-Australia ISA was signed in September 2016; the Canada-New Zealand ISA will be signed in Summer 2017; and, the Canada-UK ISA is currently under development. Note that automated exchanges of information do not occur until the regulations are in force and a bilateral arrangement is also in place.
End date (if applicable)	N/A

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

No. Information disclosed for research or statistical purposes will be in the aggregate and/or depersonalized.

Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA please contact a Research and Evaluation Division at Research-Recherche@cic.gc.ca.



22. Will a personal information bank (PIB) result from this initiative?

No new PIBs will be created as a result of this initiative.

The below-noted applicable PIBs include an indication that information may be shared with foreign governments, subject to agreement or arrangement.

- International Mobility (CIC PPU 054)
- Sponsors of Foreign Nationals (IRCC PPU 013)
- Refugee and Humanitarian Resettlement (CIC PPU 008)
- In-Canada Asylum (CIC PPU 009)
- Protected Person Status Documents (CIC PPU 066)
- Migration Control and Security Management (CIC PPU 068)
- Permanent Economic Residents (CIC PPU 042)
- International Students (CIC PPU 051)

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

Part 6 – Summary of Risks and Mitigation Strategies

23. Risk Mitigation Table

Risk Mitigation Table				
	Risk	Mitigation Strategy	Likelihood	Impact
1.	Sharing information on Canadian citizens or permanent residents: Contrary to the Regulations, Canada may provide information to an M5 partner on an individual who is either a Canadian citizen or permanent resident.	<p>Incorporating query/response rules in GCMS: A query can be sent/received only if the case type is identified. With the exception of refugee cases, it is intended that a 'no match' response will be automatically sent if a query hits against a record of a Canadian citizen or permanent resident.</p> <p>For refugee cases, Canada will respond to a match with information on permanent residents only, if available, to indicate that the individual has a durable solution in Canada, so as to uphold Canada's international commitments related to refugees.</p>	Low	High
2.	Over-collection of information: Contrary to the Regulations, Canada may use the reciprocal query process to obtain information from an M5 partner on clients, "just in case".	Limiting the use of reciprocal queries: The disclosure of information is limited to that which is necessary, relevant and proportionate to achieving the purposes of the Regulations. In the case of Canada-Australia information sharing, Canada will use the reciprocal query function only for open applications or enforcement cases, and approved asylum cases.	Low	High
3.	Uninformed disclosure of	Clear disclosure notices:	Low	Low

IRCC Privacy Impact Assessment

Migration Five Information Sharing Regulations

<p><i>information to IRCC: Clients may be unaware that Canada exchanges information with M5 partners to support the administration and enforcement of Canada's immigration laws, and M5 partners' laws in respect of citizenship and immigration.</i></p>	<p><i>Immigration application forms include a disclosure notice indicating the authority for, and purpose of, the collection of information. Disclosure notices clearly state that personal information, including immigration information related to biometric records, may be shared with foreign governments with whom Canada has an agreement or arrangement.</i></p> <p><i>An ongoing review of disclosure notices related to the Department's biometrics program will seek to ensure compliance with the Directive on Privacy Practices where gaps are identified.</i></p> <p><i>It should also be noted that existing arrangements with Australia, New Zealand and the United Kingdom are available to the public via the Department's website.</i></p>		
--	--	--	--

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

Part 7 – Executive Summary

The Migration Five (M5) is a longstanding forum for cooperation between the border and immigration agencies of Australia, Canada, New Zealand, the United Kingdom (UK), and the United States (U.S.). Given the commonalities among our immigration programs, the exchange of immigration information among M5 partners is a particularly beneficial element of this cooperation.

While manual and case-by-case information exchanges with M5 partners have proven to be a valuable tool for immigration decision-makers, the labour-intensive process involved has limited the number of cases for which information exchanges may take place.

In 2015, Canada began automated, biometric-based immigration information exchanges with the U.S., supported by regulatory amendments that were enacted to enable (though not require) these exchanges. Beginning In 2017, Canada is establishing a similar automated capability to exchange immigration information with its remaining M5 partners, namely Australia, New Zealand, and the UK.

While the M5 is a *multilateral* forum for cooperation, information exchanges between each country occur on a *bilateral* basis.

Officials in each jurisdiction can use the shared information to inform their independent admissibility decisions on the basis of their own country's immigration and refugee protection laws.

IRCC has identified three privacy risks associated with automated information sharing with M5 partners, and has implemented mitigation measures to address these risks.


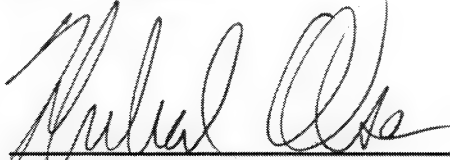
Scope of the PIA

The scope of this Privacy Impact Assessment (PIA) Report is limited to the regulations establishing the regulatory framework for automated biometric-based immigration information sharing with Australia, New Zealand, and the UK. The regulations in question can be found in Division 3 of Part 19.1 of the Immigration and Refugee Protection Regulations, beginning at Section 315.36.

IRCC Privacy Impact Assessment Five Country Conference Information Sharing Regulations

Part 8 – Corporate Affairs, ATIP Division Comments and Signatures

This PIA is based on a review of the material provided to Corporate Affairs, ATIP Division, and the OPC as of the date below. If, in future any substantive changes are made to the scope of this PIA, the Department will complete a PIA Update and submit it to ATIP Division and the OPC.

<u>AUDREY WHITE</u> Director ATIP Division	<u></u> Signature	<u>6-9-2017</u> Date
<u></u> Director General Corporate Affairs	<u>MICHAEL OLSEN</u> Signature	<u>15 June 2017</u> Date

IRCC Privacy Impact Assessment
Migration Five Information Sharing Regulations

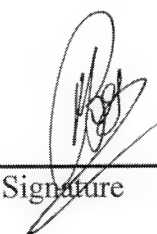
Part 9 – Program Area Comments and Signatures

Emmanuelle Deault-Bonin
Program Lead
Director


Signature

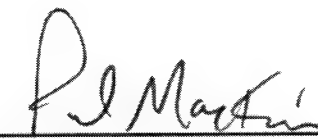
May 19, 2017
Date

Mieke Bos
Program Lead
Director General


Signature

May 24, 2017
Date

Paul MacKinnon
Program Lead
Assistant Deputy Minister

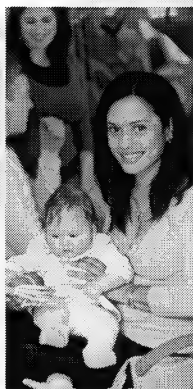

Signature

JUN 26 2017
Date



Immigration, Refugees
and Citizenship Canada

Immigration, Réfugiés
et Citoyenneté Canada



Privacy Impact Assessment

Migration Five Information Sharing Regulations



Immigration, Refugees and Citizenship Canada



IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

Name of Branch/Division:	Admissibility – Identity Management and Information Sharing		
PIA Drafter:	Brad Adams-Barrie		
Email:	Bradley.Adams-Barrie@cic.gc.ca	Phone:	613-437-7890
Program Manager:	Emmanuelle Deault-Bonin		
Email:	Emmanuelle.Deault-Bonin@cic.gc.ca	Phone:	613-437-5894

Part 1 – General Information

1. Description of the Initiative

The Migration Five (M5) is a longstanding forum for cooperation between the border and immigration agencies of Australia, Canada, New Zealand, the United Kingdom (UK), and the United States (U.S.). Given the commonalities among our immigration programs, the exchange of immigration information among M5 partners is a particularly beneficial element of this cooperation.

While manual and case-by-case information exchanges with M5 partners have proven to be a valuable tool for immigration decision-makers, the labour-intensive process involved has limited the number of cases for which information exchanges may take place. These manual, case-by-case exchanges are undertaken pursuant to section 8(2) of the *Privacy Act*, as well as case-by-case arrangements with each M5 partner.

In 2015, Canada began automated, biometric-based immigration information exchanges with the U.S., supported by regulatory amendments that were enacted to enable (though not require) these exchanges. In 2017, Canada is establishing a similar automated capability to exchange immigration information with its remaining M5 partners, namely Australia, New Zealand, and the UK. This Privacy Impact Assessment (PIA) covers the regulatory amendments that have been brought forward to provide a reasonable lawful authority for biometric-based immigration information sharing with these three partners.

While the M5 is a *multilateral* forum for cooperation, information exchanges between each country occur on a *bilateral* basis. Automated biometric-based immigration information sharing refers to an automated query and response process whereby the exchange of information is triggered when either Canada or an M5 partner sends a client's encrypted and otherwise anonymous fingerprints, plus the case type (*e.g.*, visa applicant, refugee claimant, etc.) to the

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

other country. The case type is included as part of the query to enable the exchange of information on permanent residents for refugee cases only. Under no circumstance will the client's identity be disclosed as part of the query. The country receiving the query will search its relevant database for a fingerprint match. Regardless of the result (*i.e.*, whether or not there is a match), the receiving country will automatically and immediately delete the encrypted fingerprints used in a query. In the case of a match, the receiving country will reply with limited and agreed-to data elements, consisting of biographic identity information and immigration information. Officials in each jurisdiction can use the shared information to inform their independent admissibility decisions on the basis of their own country's immigration and refugee protection laws.

For Canada, fingerprint queries will be submitted to an M5 partner to support an examination or determination following an application or claim made by a national of a third country for a permanent or temporary resident visa, a work or study permit, protection, refugee protection or any other immigration benefit, or to determine whether the national of a third country is authorized to travel to, enter or remain in Canada (Sub-section 315.4(1) of the Regulations). It is expected that Canada will have the ability to send up to 400,000 queries per year to each of these three countries, for a total of 1.2 million queries per year. It is important to note that while these regulations enable automated information sharing, they do not create a requirement to share information.

At the same time, M5 partners will query Canada for similar purposes, and Canada will disclose information in response to a query in order to support an M5 partner's examination or determination following an application or claim made by a national of a third country for a visa or immigration-related permit, status or benefit, or to determine whether the national of a third country is authorized to travel to, enter or remain in the M5 partner's territory (Paragraphs 315.41.1(a) and (b) of the Regulations). It is expected that each of these three countries will have the ability to send Canada up to 400,000 queries per year.

Canada will not disclose information on Canadian citizens. However, in order to uphold Canada's international commitments related to refugees, Canada may disclose information on Canadian permanent residents only in response to a query on a refugee case, to indicate to a partner that the individual in question has a durable solution in Canada. (Paragraph 315.41(1)(d) of the Regulations).

2. Scope of this Privacy Impact Assessment

This PIA covers automated, biometric-based immigration information sharing with Australia, New Zealand, and the UK, as enabled by amendments to the *Immigration and Refugee Protection Regulations* (IRPR). For ease of reference, the regulatory authority for this information sharing can be found beginning at Section 315.36 of the IRPR.

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

As the Regulations apply to automated biometric-based immigration information sharing with these three countries, separate PIAs will not be developed for each of the Automated Annexes to the Memoranda of Understanding (MOU) with each M5 partner, as the information sharing activities thereunder are governed by the Regulations. If, during negotiations, significant differences arise in either the contemplated exchange of information between Canada and an M5 partner, or the specific data being exchanged between Canada and an M5 partner, addenda to this PIA will be provided in order to account for notable differences.

This PIA does not cover:

- the storage of information in Immigration, Refugees and Citizenship Canada's (IRCC) Global Case Management System (GCMS), for which a PIA was submitted in 2011;
- the MOUs with Australia, New Zealand or the UK, nor the related Case-by-Case Annexes, for which PIAs were submitted in 2015 for the UK and 2016 for Australia and New Zealand;
- the High Value Data Sharing Protocol, for which a PIA was submitted in 2012; or,
- the role of the Royal Canadian Mounted Police (RCMP) as the service provider for IRCC's biometric program, for which the RCMP will submit a PIA in 2017.

3. Legal Authorities

The legislative authority for establishing information sharing regulations is:

Immigration and Refugee Protection Act

Sub-paragraphs 150.1(1)(a) and 150.1(1)(b)

150.1 (1) The regulations may provide for any matter relating to

- (a) the collection, retention, use, disclosure and disposal of information, including a Social Insurance Number, for the purposes of this Act or for the purposes of program legislation as defined in section 2 of the Canada Border Services Agency Act;
- (b) the disclosure of information for the purposes of national security, the defence of Canada or the conduct of international affairs, including the implementation of an agreement or arrangement entered into under section 5 or 5.1 of the Department of Citizenship and Immigration Act or section 13 of the Canada Border Services Agency Act;

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

4. Related Privacy Impact Assessments

The operational and technical infrastructure being developed to support information sharing with M5 partners is as described in the *Addendum Privacy Impact Assessment Report covering Biometric Systematic Information Sharing between Canada and the United States*, which was submitted to the Office of the Privacy Commissioner in May 2015.

At this time, there is one substantive privacy-linked difference between the existing automated biometric-based information sharing program in place with the United States and the program being established with the remaining M5 partners.

Specifically, Australia's Department of Immigration and Border Protection has expressed an interest in querying Australian citizenship applicants against Canada's immigration-related biometric records. This means that Canada may provide limited immigration information to Australia on a national of a third country that would be used by Australia to support a citizenship-related examination or determination. This variance is captured at Paragraph 315.41(1)(c) of the regulations.

For clarity, Canada will not send queries to M5 partners on individuals applying for Canadian citizenship.

5. Elements of Information or Data

When querying an M5 partner, IRCC will submit the person's fingerprints accompanied by a unique transaction number (Section 315.38 of the Regulations).

In the event that a query received from an M5 partner results in a fingerprint match in Canada's immigration-related biometric database, Canada will disclose:

- the individual's biographic data, such as last name, first name, date of birth, gender and country of birth;
- their photograph; and,
- information related to the administration and enforcement of Canada's immigration laws, including the issuing country of the individual's passport, the individual's immigration status, information relevant to – and any previous decision or determination relating to – their admissibility, and any decision or determination relating to a claim for refugee protection or an application for protection (Paragraphs 315.41(2)(a), 315.41(2)(b), and 315.41(2)(c) of the Regulations).

As described in section 4, Australia's Department of Immigration and Border Protection has expressed an interest in querying Australian citizenship applicants against Canada's immigration-related biometric records. This means that Canada may provide limited immigration information to Australia on a national of a third country which would be used in supporting a citizenship-

IRCC Privacy Impact Assessment

Migration Five Information Sharing Regulations

related examination or determination (Paragraph 315.41(1)(c) of the Regulations). Canada will not send queries to M5 partners on individuals applying for Canadian citizenship.

While the regulations list the information categories that may be disclosed by Canada, the following exhaustive list of data elements may be provided in response to all biometric matches, subject to availability. To note, business rules in GCMS preclude disclosures described in paragraph 315.41(3) of the regulations, i.e., disclosures inconsistent with domestic law or national interests.

Data Element	Description	Rationale for Collection
Providing Participant subject specific reference number	A unique reference number by which the client is known in the providing country.	Information is collected for reference purposes and/or in the event there is a need to recall a client's case file for the purposes of correction or initiating a Q3.
Providing Participant event specific reference number	A unique reference number for each recording event pertaining to the matched client.	
Name(s)	Biographic information and a facial image collected by a Migration 5 partner in a previous encounter with the client.	Authorized officers may verify identity information provided as part of an application with information provided by the same individual in a previous encounter with a Migration 5 partner.
Alias(es)		
Gender		
Photograph/Facial Image		
Date of Birth		
Passport Nationality or Nationalities		
Country of Birth		
Travel Document Information, including scans of documents		Significant discrepancies between information provided by the client to the Department and that which was provided to Migration 5 partners may indicate an attempt to conceal an identity, and may lead to a potential inadmissibility for misrepresentation (s. 40 of <i>Immigration and Refugee Protection Act</i>).
Current and Previous immigration status	Description of client's current or previous immigration status with a Migration 5 partner.	Information may be used to verify immigration history provided as part of an application. Significant discrepancies may also indicate a potential inadmissibility for

IRCC Privacy Impact Assessment

Migration Five Information Sharing Regulations

		<p>misrepresentation.</p> <p>Information may serve as an indicator of a client's risk of non-compliance with a program's requirements (e.g., risk of overstaying a visa).</p>
Location(s), date(s) and reason(s) fingerprinted	Information on the location, date and reason for fingerprinting a client during a previous encounter with a Migration 5 partner.	<p>Information may be used to verify immigration history.</p> <p>Information may serve as an indicator of a client's risk of non-compliance with a program's requirements (e.g., risk of overstaying a visa).</p>
Country of Alleged Persecution	Where a client has previously claimed asylum in a Migration 5 partner, the country where client has claimed alleged persecution.	Information may be used to verify information provided in an application or a refugee basis of claim. This information may have a bearing on an eligibility or admissibility determination depending on the type of application submitted.
Reason for Alert	The reason why the client is on an immigration watchlist.	Information could alert processing officers to a potential inadmissibility (s. 34-38 of <i>Immigration and Refugee Protection Act</i>)
Visa Refusal Code	A code used by a Migration 5 partner to indicate a reason for refusing a visa to client in a previous encounter.	Processing officers may use this information to verify information provided as part of an application, or to inform an eligibility or admissibility determination depending on the type of application submitted.
Watchlist indicator	Codes used to flag potential risks. May warrant further investigation.	Information provided in this field could alert processing officers to a potential

IRCC Privacy Impact Assessment

Migration Five Information Sharing Regulations

		inadmissibility (s. 34-38 of <i>Immigration and Refugee Protection Act</i>)
Date(s) and location(s) of arrival	Where a client has previously visited a Migration 5 partner, a description of the length stay and the locations from which the client arrived and departed.	<p>Information could indicate a client's non-compliance (or compliance) with length of stay requirements.</p> <p>Information may also be used to verify a client's travel history, which may inform an eligibility or admissibility determination.</p>
Date(s) and location(s) of departure		
Date removed	Where a client has been previously removed from a Migration 5 partner, a description of the date of removal.	Processing officers can use this information to verify immigration history and may indicate a potential inadmissibility.
Status of Refugee Claim	Where a client has previously claimed asylum, a description of the status of their claim.	Processing officers may use this information to verify information provided in an application or a refugee basis of claim, which may have a bearing on that client's eligibility for an immigration benefit or admissibility determination.
Date(s) of immigration application	Description of the date(s) of client's previous application(s) to a Migration 5 partner.	<p>The data elements describing a client's previous immigration encounters may be used to verify information provided in an application or have a bearing on an officer's determination on eligibility or admissibility.</p> <p>Significant discrepancies may also indicate a potential inadmissibility for misrepresentation. Information may also indicate a potential inadmissibility based on</p>
Type(s) of immigration application	Description of the type(s) of application provided in a client's previous encounter(s) with a Migration 5 partner	
Date(s) of outcome of immigration application	Description of the date(s) of a determination on a client's previous encounter(s) with a Migration 5 partner.	

IRCC Privacy Impact Assessment

Migration Five Information Sharing Regulations

Outcome of immigration	Description of the outcome(s) of a client's previous encounter(s) with a Migration 5 partner.	criminality.
Reason for outcome of immigration application	Description of rationale for a determination in a client's previous encounter(s) with a Migration 5 partner.	
Expiry date of current leave/stay or visa	Where the client has been granted temporary leave or permission to stay, or has a valid visa or entry clearance, the date on which that expires.	

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

6. Storage or Access outside Canada

Information disclosed by Canada to Australia, New Zealand or the UK in response to a query will be retained in accordance with the terms of the respective MOU, Automated Annex, and Australian, New Zealand, or UK law.

Information disclosed to Australia's Department of Immigration and Border Protection will be stored in Australia's Biometric Acquisition Matching Service system.

Information disclosed to New Zealand's Ministry of Business, Innovation and Employment will be stored in New Zealand's "M5 Check" system.

The UK's Home Office is currently undertaking an overhaul of its immigration information technology systems, and automated biometric-based information sharing is not scheduled to be implemented between Canada and the UK until 2018 at the earliest. Clarification will be sought by Canada at that time as to which system the UK will store information received from Canada.

Officials in Australia, New Zealand, or the UK will not have direct access to Canadian case files, databases or other information held by IRCC, or vice versa.

The information IRCC receives from Australia, New Zealand, or the UK will be stored in GCMS, which is housed in Canada. Information may also be kept on client case files in paper format.

7. Data-matching program

Answer the following questions to determine whether your initiative qualifies as a "data-matching program". If you answer "yes" to all 3 questions, your initiative may be a data matching program.	
1. Personal information from one database is linked or combined with personal information from another database;	Yes
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	No
3. The linkage results in an administrative decision about an individual.	Yes
If you have answered "yes" to all three questions, please contact ATIP Division to discuss the requirements of a data-matching program.	

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

8. Multi-institutional/Multi-jurisdictional

Is your initiative Multi-institutional/ Multi-jurisdictional ? Will the privacy impact assessment involve more than one government institution? <i>YES – IRCC and the CBSA are both subject to the Immigration and Refugee Protection Regulations, including the information sharing regulations being examined in this PIA report.</i>	
1. This initiative involves a program or activity that provides a service (or services);	<input checked="" type="checkbox"/> Yes
2. Those services are provided through: (a) an institution and at least one other institution or department working collaboratively to provide that service; or (b) one institution working on behalf of one or more other institutions;	<input checked="" type="checkbox"/> Yes
3. The common or integrated program/activity is confirmed by written documentation.	<input checked="" type="checkbox"/> Yes
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	<input checked="" type="checkbox"/>

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

Part 2 – Protection of Personal Information

9. Personal Information Flow Diagram and/or Personal Information Flow Table

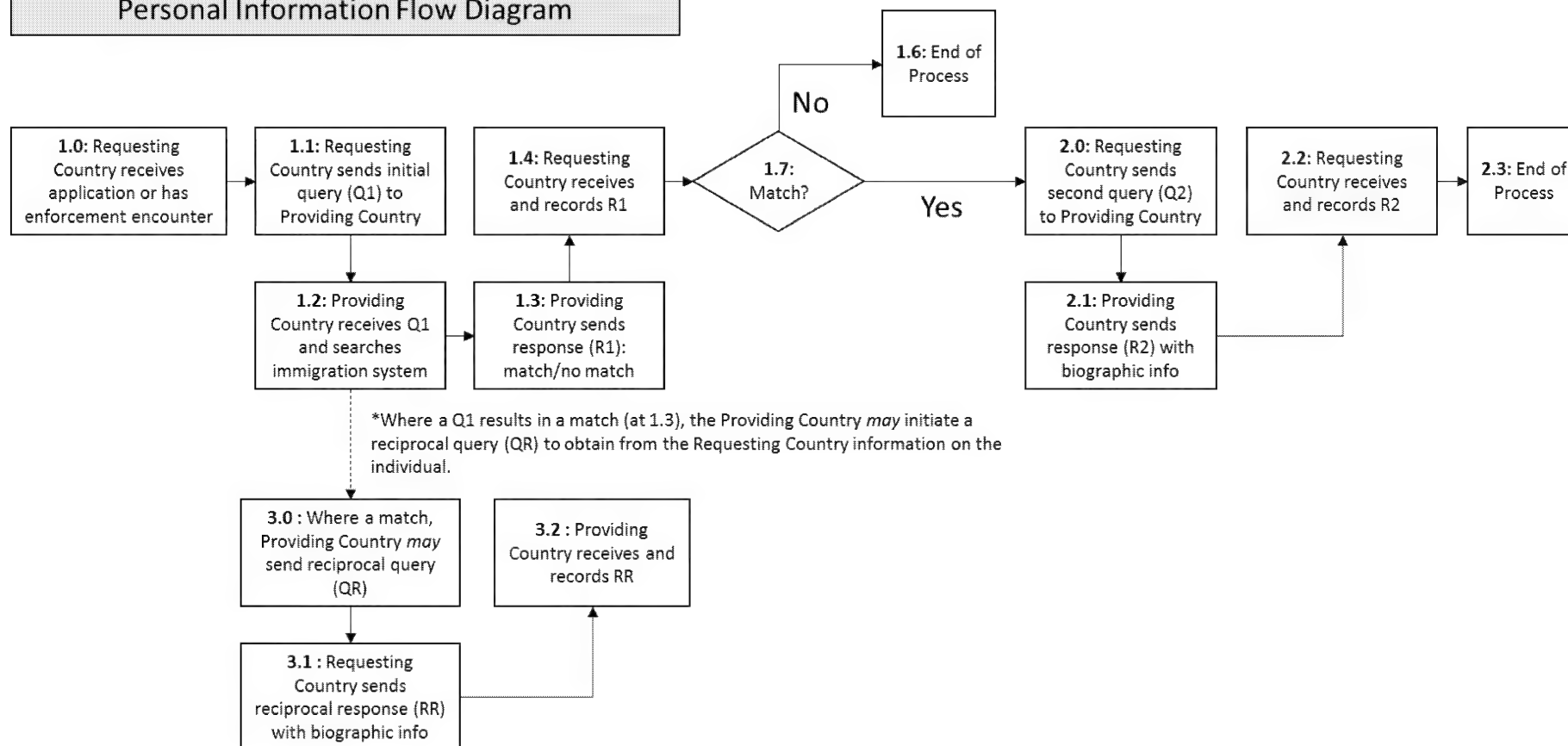
A data flow diagram is provided below outlining the automated search and response process. The following information can be used as a reading guide for the data flow diagram.

- The requesting country initiates a query using an electronic fingerprint. (see section 1.0 in data flow diagram).
- The fingerprint is searched against the providing country's applicable database.
- If a match is established, the providing country responds with biographic information (*e.g.*, name, age, nationality, etc.) and limited immigration information (*e.g.*, reason fingerprinted).
- The fingerprint is deleted by the providing country.
- Following a match, the requesting country requests additional immigration information from the providing country. (see section 2.0 in data flow diagram).
- The providing country automatically provides additional immigration information, subject to availability (*e.g.*, travel document information; application outcomes).
- The providing country can also send a "reciprocal query" in specific and limited circumstances to receive identity information and limited immigration data to assist in administering and enforcing its own immigration laws (*e.g.*, when the query hits against an open immigration warrant). (see section 3.0 in data flow diagram). Canada will only initiate a reciprocal query in the following circumstances:
 1. If a partner's query matches to an open Canadian visa application: this will assist in ensuring that the individual is providing consistent information to immigration officials in both countries and mitigate the risk of "visa shopping" using different biographic identities.
 2. If a partner's query matches to an approved asylum claim in Canada: this will assist in ensuring that an individual who has been granted asylum in Canada continues to be eligible for status in Canada. For instance, a person can have their refugee status vacated if they obtained that status by directly or indirectly misrepresenting or withholding material facts relating to a relevant matter. Reciprocal queries could reveal such information.
 3. If a partner's query matches to an open enforcement case in Canada: to ensure that Canadian officials have the most accurate and up to date information available concerning individuals who are wanted, but have yet to be removed from Canada.

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

This will also help to reduce the resource burden on enforcement officials should it be discovered that an individual wanted for removal has in fact left the country.

Automated Biometric-based Information Sharing: Personal Information Flow Diagram



IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

10. Disclosure Notice

Immigration application forms include a disclosure notice indicating the authority for, and purpose of, the collection of information and how to obtain further information on applicable Personal Information Banks. Immigration application forms also state that personal information, including immigration information related to biometric records, may be shared with foreign governments with whom Canada has an agreement or arrangement. IRCC application forms are available via the following link: <http://www.cic.gc.ca/english/information/applications/>.

Of note, IRCC is presently undertaking a review of disclosure notices on application forms linked to its biometrics program and will seek to ensure compliance with the Directive on Privacy Practices where gaps are identified.

Part 3 – Security of Personal Information

11. Describe the physical security measures related to the initiative.

Information exchanged under the regulations will be securely stored and encrypted in accordance with existing Government of Canada security procedures and standards.

12. Describe the technical security measures related to the initiative.

Encryption

Information collected from and disclosed to Australia's Department of Immigration and Border Protection, New Zealand's Ministry of Business, Innovation and Employment, or the UK's Home Office will be protected with controls and safeguards applicable to Protected 'B' information, including encryption during electronic transmission

Controlled User Access Profiles

GCMS Access Controls allow users who have the proper authorization to obtain access to specific items of information. Credentials are used to verify and authenticate the identity of these users where special permission and authorizations are required to perform tasks and processes. GCMS users are assigned access to the system by role and office based on their specific job requirements. Information received from an M5 partner is captured in a specific GCMS view, to which access is limited to IRCC and CBSA employees with an immigration case processing role. For more detailed information regarding GCMS access controls, please refer to the GCMS PIA that was submitted to the Office of the Privacy Commissioner in 2011.

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

13. Does your branch rely on security policies in addition to the TBS Policy on Government Security?

IRCC adheres to Canadian laws and policies guiding the protection of personal information. In addition to the TBS policy on Government Security, IRCC adheres to the TBS Operational Security Standard on Physical Security which provides baseline physical security requirements for the storage, transmittal, and destruction of classified and protected information. IRCC will also adhere to the CSE's *IT Security Risk Management: A Lifecycle Approach* (ITSG-33) guidelines which provide a set of clearly defined activities to ensure key steps are performed on an ongoing basis during the lifetime of the department's information systems, and to ensure risk management is applied from an enterprise perspective. Per CSE's ITSG-33 guidelines, IRCC performs the Security Assessment & Authorization (SA&A) process, resulting in a signed Authority to Operate (ATO) for every GCMS release, including those through which automated biometric-based information sharing has been or will be implemented with Australia, New Zealand and the UK.

- *Operational Security Standard on Physical Security*
<http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329§ion=text#appB>
- *IT Security Risk Management: A Lifecycle Approach (ITSG-33)*
<https://www.cse-cst.gc.ca/en/node/265/html/22814>

14. Describe any mitigating access controls to limit or restrict unauthorized access to personal information including changes such as additions or deletions.

Personal information may only be accessed by authorised individuals who have a need to access that information in performing their official duties. Only specific IRCC and CBSA officials may access information received from Australia's Department of Immigration and Border Protection, New Zealand's Ministry of Business, Innovation and Employment, or the UK's Home Office.

Exchanges will be recorded in GCMS, where additions or deletions are subject to user controls. Furthermore, all automated exchanges of information will be immediately marked and labeled on the client's file in GCMS. The special treatment of this information within GCMS will further emphasize the controlled nature of this information and more readily allow, in the case of access to information requests, for an individual to know that an information exchange was completed with Australia, New Zealand, or the UK.

15. Explain how you will identify individuals accessing personal information without authorization.

GCMS Access Controls allow users who have the proper authorization to obtain access to specific items of information. Access Control processes are in place to restrict read/write access to GCMS data (which includes any biometric related data stored in the GCMS system).

IRCC Privacy Impact Assessment

Migration Five Information Sharing Regulations

The auditing controls collect data, support analysis, and manage the archiving of all information. The auditing controls allow for the capture, analysis, and retrieval of records of events and conditions within a computing solution.

Data Auditing is divided into Write Auditing and Read Auditing. Read audit refers to the ability to capture which GCMS user has viewed data and the content of the data at that point in time. Write audit refers to the capturing of changes to data that occur within the GCMS system. The goal of the write audit is to capture what changes, additions and deletions are performed on the system, which user performed the changes and when they occurred. The write audit requirements being addressed by GCMS can be expressed as the ability to answer the following questions:

- What activity did a given user perform over a specified time period;
- What activity was performed against a given client over a specified time period; and
- What activity against a given client was performed by a given user over a specified time period?

Audit can be in real-time, such as an Intrusion Detection system, or can be after the fact, such as a scheduled periodic review of events that have been previously gathered in a log. Audit Controls include:

- collection of audit data about events, including capture of the appropriate data, trusted transfer of audit data, and synchronisation of chronologies;
- protection of security audit data, including use of time stamps, signing events, and storage integrity to prevent loss of data;
- analysis of security audit data, including review, anomaly detection, violation analysis, and attack analysis using simple or complex heuristics; and
- alarms for event or activity thresholds, warning conditions, and critical events.

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

Part 4 – Accuracy/Correction/Retention of Personal Information

- 16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the Department notify them of the update, correction or annotation?**

IRCC will use existing processes to respond to requests for access to information made under the *Access to Information Act*, and the correction of inaccurate information under the *Privacy Act*.

If an individual has a right of access to his or her information under the *Privacy Act* and makes a request regarding corrections to said information, IRCC will comply as appropriate.

If IRCC or the CBSA becomes aware that information disclosed in response to a query from an M5 partner is inaccurate, the recipient of the inaccurate information must be notified and correcting information be provided as soon as feasible (Sub-section 315.42(1) of the Regulations). Similarly, if IRCC or the CBSA receives information from an M5 partner that corrects information previously disclosed by that partner, IRCC or the CBSA must make the necessary correction as soon as is feasible and notify the partner that the correction has been made (Sub-section 315.42(2) of the Regulations).

- 17. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.**

Yes. Personal information may be used to inform immigration and refugee decisions, and in the case of Australia, decisions related to Australian citizenship applications. Biometric-based information sharing can help verify a client's identity and obtain previously unknown immigration information.

- 18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.**

Where personal information is collected directly from the client, it is incumbent on the client to provide information that is accurate and complete. When clients provide new and updated information, it can be entered and reflected in GCMS.

IRCC and its counterparts in M5 countries are committed to providing the most up to date and accurate information available. If Canada or an M5 partner becomes aware that the other is using inaccurate information, there is an obligation to notify the other immediately and provide correct information, where available. As described in section 16, Canada's obligation to correct inaccurate information disclosed in response to a query is captured in the regulations; information disclosed in either a query or response is limited to that which is necessary, relevant and proportionate to

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

achieving the purposes of the Regulations, and the information must be disclosed in a manner that ensures the accuracy and reliability of the information (Section 315.39 of the Regulations).

19. If you answered “yes” to question 17, do you have approved records retention and disposition schedules that will ensure that personal information is kept for a minimum of two years after it is used in making a decision directly affecting an individual?

Yes. Domestic retention policies and laws apply to the information exchanged under the authority of the regulations (Sub-section 315.43(1) of the Regulations, with the exception of the fingerprints used to form the query, which are always deleted by the receiving partner regardless of outcome (Sub-section 315.13(2) of the Regulations).

Information will be retained in accordance with the approved records retention and disposition schedule for the relevant application type.

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

Yes. Personal information will be disclosed in an automated and systematic manner as described in section 9.

For Canada, queries will be automated and initiated upon receipt of an application or claim for which the applicant is required to submit biometrics (i.e. fingerprints).

Canada’s responses to queries from an M5 partner will also be automated. When a fingerprint match has been established by the RCMP, IRCC will pull the limited and relevant immigration information from the client’s file in GCMS and return the data elements listed in question 5, as available, to the applicable M5 partner.

Please check this box if a related Information Sharing Agreement (ISA) has been prepared. If you have general questions about preparing an ISA, please contact your International and Intergovernmental Relations (IIR), Intergovernmental Relations (IGR) at NHQ-IGR@cic.gc.ca - or contact the ATIP division at ATIPinternal-AIPRPinterne@cic.gc.ca .



IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

If an ISA has been prepared as part of your initiative, please complete the fields in the table below.

Information Sharing Agreement – Required Information	
Description	<p>Annex to the Memorandum of Understanding between the Department of Citizenship and Immigration Canada and the Canada Border Services Agency and the Department of Immigration and Border Protection of Australia regarding the Exchange of Information on an Automated Basis;</p> <p>Annex to the Memorandum of Understanding between the Department of Citizenship and Immigration Canada and the Canada Border Services Agency and New Zealand's Ministry of Business, Innovation, and Employment (Immigration New Zealand) regarding the Exchange of Information on an Automated Basis.</p> <p><i>N.B.:</i> A Canada-UK Annex for the automated exchange of information is currently under development.</p>
Primary government institution involved	IRCC and CBSA and, on a bilateral basis, Australia's Department of Immigration and Border Protection & New Zealand's Ministry of Business, Innovation and Employment, and the UK's Home Office.
All other government institution and/or parties involved	N/A
ISA contact title	IRCC – Emmanuelle Deault-Bonin, A/Director, Identity Management and Information Sharing CBSA – Sébastien Aubertin-Giguère, A/Director General, Traveller Program Directorate
ISA contact telephone number	Emmanuelle Deault-Bonin: 613-437-5894 Sébastien Aubertin-Giguère: 613-952-3266
Indication of whether or not personal	Yes, the exchange of personal information is

IRCC Privacy Impact Assessment

Migration Five Information Sharing Regulations

information is involved	involved in this arrangement.
Start date	The Canada-Australia ISA was signed in September 2016; the Canada-New Zealand ISA will be signed in Summer 2017; and, the Canada-UK ISA is currently under development. Note that automated exchanges of information do not occur until the regulations are in force and a bilateral arrangement is also in place.
End date (if applicable)	N/A

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

No. Information disclosed for research or statistical purposes will be in the aggregate and/or depersonalized.

Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA please contact a Research and Evaluation Division at Research-Recherche@cic.gc.ca.

☐

22. Will a personal information bank (PIB) result from this initiative?

No new PIBs will be created as a result of this initiative.

The below-noted applicable PIBs include an indication that information may be shared with foreign governments, subject to agreement or arrangement.

- International Mobility (CIC PPU 054)
- Sponsors of Foreign Nationals (IRCC PPU 013)
- Refugee and Humanitarian Resettlement (CIC PPU 008)
- In-Canada Asylum (CIC PPU 009)
- Protected Person Status Documents (CIC PPU 066)
- Migration Control and Security Management (CIC PPU 068)
- Permanent Economic Residents (CIC PPU 042)
- International Students (CIC PPU 051)

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

Part 6 – Summary of Risks and Mitigation Strategies

23. Risk Mitigation Table

Risk Mitigation Table				
	Risk	Mitigation Strategy	Likelihood	Impact
1.	Sharing information on Canadian citizens or permanent residents: Contrary to the Regulations, Canada may provide information to an M5 partner on an individual who is either a Canadian citizen or permanent resident.	<p>Incorporating query/response rules in GCMS: A query can be sent/received only if the case type is identified. With the exception of refugee cases, it is intended that a 'no match' response will be automatically sent if a query hits against a record of a Canadian citizen or permanent resident.</p> <p>For refugee cases, Canada will respond to a match with information on permanent residents only, if available, to indicate that the individual has a durable solution in Canada, so as to uphold Canada's international commitments related to refugees.</p>	Low	High
2.	Over-collection of information: Contrary to the Regulations, Canada may use the reciprocal query process to obtain information from an M5 partner on clients, "just in case".	Limiting the use of reciprocal queries: The disclosure of information is limited to that which is necessary, relevant and proportionate to achieving the purposes of the Regulations. In the case of Canada-Australia information sharing, Canada will use the reciprocal query function only for open applications or enforcement cases, and approved asylum cases.	Low	High
3.	Uninformed disclosure of	Clear disclosure notices:	Low	Low

IRCC Privacy Impact Assessment

Migration Five Information Sharing Regulations

<p>information to IRCC: Clients may be unaware that Canada exchanges information with M5 partners to support the administration and enforcement of Canada’s immigration laws, and M5 partners’ laws in respect of citizenship and immigration.</p>	<p>Immigration application forms include a disclosure notice indicating the authority for, and purpose of, the collection of information. Disclosure notices clearly state that personal information, including immigration information related to biometric records, may be shared with foreign governments with whom Canada has an agreement or arrangement.</p> <p>An ongoing review of disclosure notices related to the Department’s biometrics program will seek to ensure compliance with the Directive on Privacy Practices where gaps are identified.</p> <p>It should also be noted that existing arrangements with Australia, New Zealand and the United Kingdom are available to the public via the Department’s website.</p>		
---	---	--	--

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

Part 7 – Executive Summary

The Migration Five (M5) is a longstanding forum for cooperation between the border and immigration agencies of Australia, Canada, New Zealand, the United Kingdom (UK), and the United States (U.S.). Given the commonalities among our immigration programs, the exchange of immigration information among M5 partners is a particularly beneficial element of this cooperation.

While manual and case-by-case information exchanges with M5 partners have proven to be a valuable tool for immigration decision-makers, the labour-intensive process involved has limited the number of cases for which information exchanges may take place.

In 2015, Canada began automated, biometric-based immigration information exchanges with the U.S., supported by regulatory amendments that were enacted to enable (though not require) these exchanges. Beginning In 2017, Canada is establishing a similar automated capability to exchange immigration information with its remaining M5 partners, namely Australia, New Zealand, and the UK.

While the M5 is a *multilateral* forum for cooperation, information exchanges between each country occur on a *bilateral* basis.

Officials in each jurisdiction can use the shared information to inform their independent admissibility decisions on the basis of their own country's immigration and refugee protection laws.

IRCC has identified three privacy risks associated with automated information sharing with M5 partners, and has implemented mitigation measures to address these risks.

Scope of the PIA

The scope of this Privacy Impact Assessment (PIA) Report is limited to the regulations establishing the regulatory framework for automated biometric-based immigration information sharing with Australia, New Zealand, and the UK. The regulations in question can be found in Division 3 of Part 19.1 of the Immigration and Refugee Protection Regulations, beginning at Section 315.36.

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

Part 8 – Corporate Affairs, ATIP Division Comments and Signatures

This PIA is based on a review of the material provided to Corporate Affairs, ATIP Division, and the OPC as of the date below. If, in future any substantive changes are made to the scope of this PIA, the Department will complete a PIA Update and submit it to ATIP Division and the OPC.

Director
ATIP

Signature

Date

Director General
Corporate Affairs

Signature

Date

IRCC Privacy Impact Assessment Migration Five Information Sharing Regulations

Part 9 – Program Area Comments and Signatures

Emmanuelle Deault-Bonin

Program Lead
Director

Signature

Date

Mieke Bos

Program Lead
Director General

Signature

Date

Paul MacKinnon

Program Lead
Assistant Deputy Minister

Signature

Date